UNITED STATES DISTRICT COURT

for the

Western District of Washington

In the matter of the Search of	)	
	)	
Information Stored by Google	)	Case No. MJ23-276
	)	
	)	

APPLICATION FOR A GEOFENCE SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the person or property described in Attachment A, located in the Northern District of California, there is now concealed property and evidence described in Attachment B. This court has authority to issue this warrant under 18 U.S.C. §§ 2703(c)(1)(A) and 2711(3)(A).

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 111(a)(1)	Assault or interference with federal officer

The application is based on the facts set forth in the attached affidavit, which is incorporated herein by reference with all attachments and exhibits.

Pursuant to Fed. R. Crim. P. 41, this warrant is presented by:
☒ by reliable electronic means; or ☐ telephonically recorded

Applicant's signature

Emily Moore, Special Agent
Printed name and title

☐ The foregoing affidavit was sworn before me and signed in my presence, or
☒ The above-named officer provided a sworn statement attesting to the truth or the foregoing affidavit by telephone/

Date: June 2, 2023

Judge's signature

City and state: Seattle, Washington

BRIAN A. TSUCHIDA, United States Magistrate Judge
Printed name and title

STATE OF WASHINGTON)
) ss
COUNTY OF KING)

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A GEOFENCE SEARCH WARRANT

I, Emily Moore, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a warrant to search information that is stored at premises controlled by Google LLC, an electronic communication service and remote computing service provider headquartered in Mountain View, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a warrant under 18 U.S.C. § 2703(c)(1)(A) to require Google to disclose to the government the information further described in Attachment B.I. The government will then review that information and seize the information that is further described in Attachment B.II.

2. I am employed as a Special Agent (SA) with the Federal Bureau of Investigation (FBI) and have been employed with the FBI since October 2019. I am currently assigned to the Seattle Field Division where I am a member of the Violent Crime, Gang, and Transnational Organized Crime – Western Hemisphere squad. Prior to becoming a Special Agent with the FBI, I was a sworn Law Enforcement Officer with the Orlando Police Department in Orlando, Florida from 2016 to 2019. During this time, I served as a Patrol Officer where I participated in numerous narcotics and violent crime investigations as the primary investigator or in a subsidiary role. I have encountered and have become familiar with various tools, methods, trends, and related articles utilized by various

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

individuals in their efforts to conceal criminal activity, while enforcing state laws in that capacity. I also hold a Master of Science degree in Criminal Justice from the University of Central Florida.

3. In my role as a Special Agent for the FBI, I have responded to bank robberies and have worked with county and municipal agencies on these investigations. I have been involved in the service of federal and state search warrants and have become familiar with the manner in which criminals plan and conduct their unlawful operations.

4. I am an investigative law enforcement officer of the United States within the meaning of 18 U.S.C. § 2510(7). As such, I am empowered to conduct investigations of, and to make arrests for, violations of Title 18, United States Code, Section 922, and related offenses.

5. The facts set forth in this Affidavit are based on my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other law enforcement personnel; review of documents and records related to this investigation; communications with others who have personal knowledge of the events and circumstances described herein; and information gained through my training and experience. Because this Affidavit is submitted for the purpose of establishing probable cause for this affidavit and thus does not include each and every fact known to me concerning this investigation.

6. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. 111 (a)(1) have been committed. This statute states that "[w]hoever forcibly assaults, resists, opposes, impedes, intimidates, or interferes with any person designated in section 1114 of this title while engaged in or on account of the performance of official duties" has committed a criminal offense. There is also probable cause to search the information described in Attachment A for evidence of these crimes further described in Attachments B.I. and B.II.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

JURISDICTION

7. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

BACKGROUND RELATING TO GOOGLE AND RELEVANT TECHNOLOGY

8. Based on my training and experience, I know that cellular devices, such as mobile telephones, are wireless devices that enable their users to send or receive wire and/or electronic communications using the networks provided by cellular service providers. Using cellular networks, users of many cellular devices can send and receive communications over the Internet.

9. I also know that many devices, including but not limited to cellular devices, have the ability to connect to wireless Internet ("wi-fi") access points if the user enables wi-fi connectivity. These devices can, in such cases, enable their users to send or receive wire and/or electronic communications via the wi-fi network. A tablet such as an iPad is an example of a device that may not have cellular service but that could connect to the Internet via wi-fi. Wi-fi access points, such as those created through the use of a router and offered in places like homes, hotels, airports, and coffee shops, are identified by a service set identifier ("SSID") that functions as the name of the wi-fi network. In general, devices with wi-fi capability routinely scan their environment to determine what wi-fi access points are within range and will display the names of networks within range under the device's wi-fi settings.

10. Based on my training and experience, I also know that many devices, including many cellular and mobile devices, feature Bluetooth functionality. Bluetooth allows for short-range wireless connections between devices, such as between a device such as a cellular phone or tablet and Bluetooth-enabled headphones. Bluetooth uses radio waves

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

to allow the devices to exchange information. When Bluetooth is enabled, a device routinely scans its environment to identify Bluetooth devices, which emit beacons that can be detected by devices within the Bluetooth device's transmission range, to which it might connect.

11. Based on my training and experience, I also know that many cellular devices, such as mobile telephones, include global positioning system ("GPS") technology. Using this technology, the device can determine its precise geographical coordinates. If permitted by the user, this information is often used by apps installed on a device as part of the apps' operation.

12. Based on my training and experience, I know Google is a company that, among other things, offers an operating system ("OS") for mobile devices, including cellular phones, known as Android. Nearly every device using the Android operating system has an associated Google account, and users are prompted to add a Google account when they first turn on a new Android device.

13. In addition, based on my training and experience, I know that Google offers numerous apps and online-based services, including messaging and calling (*e.g.,* Gmail, Hangouts, Duo, Voice), navigation (Maps), search engine (Google Search), and file creation, storage, and sharing (*e.g.*, Drive, Keep, Photos, and YouTube). Many of these services are accessible only to users who have signed in to their Google accounts. An individual can obtain a Google account by registering with Google, and the account identifier typically is in the form of a Gmail address (*e.g.*, example@gmail.com). Other services, such as Maps and YouTube, can be used with limited functionality without the user being signed in to a Google account.

14. Based on my training and experience, I also know Google offers an Internet browser known as Chrome that can be used on both computers and mobile devices. A user has the ability to sign-in to a Google account while using Chrome, which allows the user's

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

bookmarks, browsing history, and other settings to be uploaded to Google and then synced across the various devices on which the subscriber may use the Chrome browsing software, although Chrome can also be used without signing into a Google account. Chrome is not limited to mobile devices running the Android operating system and can also be installed and used on Apple devices and Windows computers, among others.

15. Based on my training and experience, I know that, in the context of mobile devices, Google's cloud-based services can be accessed either via the device's Internet browser or via apps offered by Google that have been downloaded onto the device. Google apps, including Gmail and the others identified above, exist for, and can be downloaded to, devices that do not run the Android operating system, such as Apple devices.

16. According to my training and experience, as well as open-source materials published by Google, I know that Google offers accountholders a service called "Location History," which authorizes Google, when certain prerequisites are satisfied, to collect and retain a record of the locations where Google calculated a device to be based on information transmitted to Google by the device. That Location History is stored on Google servers, and it is associated with the Google account that is associated with the device. Each accountholder may view their Location History and may delete all or part of it at any time.

17. Based on my training and experience, I know that the location information collected by Google and stored within an account's Location History is derived from sources including GPS data and information about the wi-fi access points and Bluetooth beacons within range of the device. Google uses this information to calculate the device's estimated latitude and longitude, which varies in its accuracy depending on the source of the data. Google records the margin of error for its calculation as to the location of a device as a meter radius, referred to by Google as a "maps display radius," for each latitude and longitude point.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

18. Based on open-source materials published by Google and my training and experience, I know that Location History is not turned on by default. A Google accountholder must opt-in to Location History and must enable location reporting with respect to each specific device and application on which they use their Google account in order for that usage to be recorded in Location History. A Google accountholder can also prevent additional Location History records from being created at any time by turning off the Location History setting for their Google account or by disabling location reporting for a particular device or Google application. When Location History is enabled, however, Google collects and retains location data for each device with Location Services enabled, associates it with the relevant Google account, and then uses this information for various purposes, including to tailor search results based on the user's location, to determine the user's location when Google Maps is used, and to provide location-based advertising.

19. Location data, such as the location data in the possession of Google in the form of its users' Location Histories, can assist in a criminal investigation in various ways. As relevant here, I know based on my training and experience that Google has the ability to determine, based on location data collected and retained via the use of Google products as described above, devices that were likely in a particular geographic area during a particular time frame and to determine which Google account(s) those devices are associated with. Among other things, this information can indicate that a Google accountholder was near a given location at a time relevant to the criminal investigation by showing that his/her device reported being there.

20. Based on my training and experience, I know that when individuals register with Google for an account, Google asks subscribers to provide certain personal identifying information. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number).

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provide clues to their identity, location, or illicit activities.

21. Based on my training and experience, I also know that Google typically retains and can provide certain transactional information about the creation and use of each account on its system. This information can include the date on which the account was created, the length of service, records of login (*i.e.,* session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, Google often has records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the account.

PROBABLE CAUSE

22. From law enforcement reports, witness interviews, and surveillance video, I know that, on April 25, 2023, at approximately 8:45 p.m., at a residence in Seattle, Washington, an Assistant United States Attorney (the "AUSA") was in her home with relatives. At this time an unknown person kicked her front door so forcefully that the door jamb was damaged to the extent that the door could not be secured. The AUSA's husband was just a few feet from the front door when this occurred. The husband yelled at the perpetrator in attempts to prevent the person from coming in. After not hearing anything further, the husband looked though the peephole to the door but did not see any suspects or suspicious vehicles.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

23. Law enforcement obtained a surveillance video from a neighbor. I have seen the video. The video shows two vehicles drive onto the street where the AUSA resides. The vehicle pauses in front of the neighbor's home. The driver, who appears female, opens her door which illuminates the cab of the vehicle. Three people are seen inside the vehicle and appear to be adjusting their positions, preparing for the pending offense. The vehicle moves forward out of view of the camera with its brake lights on, suggesting that it will stop. A second vehicle is seen following the first and stops in the street. Two people run from the direction of the first vehicle up to the porches of the AUSA's house and her next-door neighbor. The person at the AUSA's house kicks the front door forcefully. The person at next-door neighbor's house seems to watch the other suspect, but does not take any action. Both suspects run away at the same time towards the first vehicle, and the vehicles drive away.

24. Based on my investigation, there is probable cause to believe that the AUSA was targeted on account of her official duties.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

28. There is also evidence that someone seeking to retaliate against the AUSA mistakenly targeted one of the AUSA's relatives. The AUSA has a relative with the same first and last name who lives in California. From talking to the AUSA, and from law enforcement reports, I know that the relative's home was broken into on April 21, 2023 – four days before the AUSA's door was kicked in. The house was unoccupied. The front door had been broken open. The intruder or intruders took a wedding album, family keepsakes, and jewelry, but left valuable electronics behind.

29. Investigators have not yet been able to identify the person who kicked in the AUSA's door. Based on what we have learned from the investigation, and my training and experience, there is probable cause to believe that the information sought by this application could help identify the suspect and any associates. People commonly carry cellular devices on their person or vehicles, and those devices are often associated with Google accounts. If

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

the suspects possessed a Google-associated device, or a device with Google apps, within the search parameters, the requested warrant could provide valuable identifying information.

30. Based on the foregoing, I submit that there is probable cause to search information that is currently in the possession of Google and that relates to the devices that reported being within the Target Location described in Attachment A[2] during the time period described in Attachment A for evidence of the crimes under investigation. The information to be searched includes (1) identifiers of each device; (2) the location(s) reported by each device to Google and the associated timestamp; and (3) basic subscriber information for the Google account(s) associated with each device.

31. The proposed warrant sets forth a multi-step process whereby the government will obtain the information described above. Specifically, as described in Attachment B.I:

a. Using Location History data, Google will identify those devices that it calculated were or could have been (based on the associated margin of error for the estimated latitude/longitude point) within the Target Location described in Attachment A during the time period described in Attachment A. For each device, Google will provide a anonymized identifier, known as a Reverse Location Obfuscation Identifier ("RLOI"), that Google creates and assigns to device for purposes of responding to this search warrant; Google will also provide each device's location coordinates along with the associated timestamp(s), margin(s) of error for the coordinates (*i.e,.* "maps display radius"), and source(s) from which the location data was derived (*e.g.*, GPS, wi-fi, bluetooth), if available. Google will not, in this step, provide the Google account identifiers (*e.g.,* example@gmail.com) associated with the devices or basic subscriber information for those accounts to the government.

The government shall review the Device List and rule out any devices that are unlikely to be related to the investigation based on timing and location information, keeping

[2] The AUSA's address is included in the information accompanying the satellite photo and coordinates included in Attachment A.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

in mind that the accuracy of location information that Google provides can vary from device to device and that it may not be possible to rule out a device based on timing and location information alone. For example, law enforcement may remove devices were moving through the Target Location(s) in a manner inconsistent with the facts of the underlying case, or for similar reasons appear not to be relevant to the investigation. After ruling out those devices (if any) that are unlikely to be related to the investigation, the government shall identify to Google the devices about which it seeks to obtain Google account identifiers and basic subscriber information.

If additional location information for a given device ID is needed in order to determine whether that device is relevant to the investigation, law enforcement will request a further search warrant that will require Google to provide additional data for time period(s) and locations that fall outside of the Search Parameter(s).

Google will then disclose to the government the Google account identifier associated with the devices identified by the government, along with basic subscriber information for those accounts.

32. This process furthers efficiency and privacy by allowing for the possibility that the government, upon reviewing contextual information for all devices identified by Google, may be able to determine that one or more devices associated with a Google account (and the associated basic subscriber information) are likely to be of heightened evidentiary value and warrant further investigation before the records of other accounts in use in the area are disclosed to the government.

33. **The proposed warrant would not authorize the disclosure or seizure of any email communications or messages (SMS text or Google chat).**

CONCLUSION

34. Based on the foregoing, I request that the Court issue the proposed warrant, pursuant to 18 U.S.C. § 2703(c).

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

35. I further request that the Court direct Google to disclose to the government any information described in Section I of Attachment B that is within its possession, custody, or control. Because the warrant will be served on Google, which will then compile the requested records at a time convenient to it, good cause exists to permit the execution of the requested warrant at any time in the day or night.

EMILY MOORE
Special Agent
Federal Bureau of Investigation (FBI)

The above-named agent provided a sworn statement to the truth of the foregoing affidavit by telephone on 2nd day of June, 2023.

BRIAN A. TSUCHIDA
United States Magistrate Judge

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A

Property To Be Searched

This warrant is directed to Google LLC, an electronic communication service and remote computing service provider headquartered in Mountain View, California, and applies to:

1. Location History data, sourced from information including GPS data and information about visible wi-fi points and Bluetooth beacons transmitted from devices to Google, reflecting devices that Google calculates were or could have been (as indicated by margin of error, *i.e.,* "maps display radius") located within the geographical region bounded by the latitudinal and longitudinal coordinates, dates, and times below ("Initial Search Parameters"); and

2. Identifying information for Google Accounts associated with the responsive Location History data.

Initial Search Parameters

- Date: April 25, 2023
- Time Period: PDT 8:30 pm to 9:00 pm
- Target Location: Geographical area identified as

- Time Restriction: Devices that reported their location more than once within the Target Location on the date and during the time period above and where at least twenty minutes elapsed between the time that the first time the device reported its location and the last time that the device reported its location.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B

Particular Items to Be Seized

I. Information to be disclosed by Google

The information described in Attachment A, via the following process:

1. Google shall query location history data based on the Initial Search Parameters specified in Attachment A. For each location point recorded within the Initial Search Parameters, and for each location point recorded outside the Initial Search Parameters where the margin of error (*i.e.*, "maps display radius") would permit the device to be located within the Initial Search Parameters, Google shall produce to the government information specifying the corresponding unique device ID, timestamp, location coordinates, display radius, and data source, if available (the "Device List").

2. The government shall review the Device List and rule out any devices that law enforcement believes are unlikely to be related to the investigation based on timing and location information, keeping in mind that the accuracy of location information that Google provides can vary from device to device and that it may not be possible to rule out a device based on timing and location information alone. For example, law enforcement may remove devices that were moving through the Target Location(s) in a manner inconsistent with the facts of the underlying case, or for similar reasons appear not to be relevant to the investigation. After ruling out those devices (if any) that law enforcement believe are unlikely to be related to the investigation, the government shall identify to Google the devices about which it seeks to obtain Google account identifier and basic subscriber information.

3. If additional location information for a given device ID is needed in order to determine whether that device is relevant to the investigation, law enforcement will request a further search warrant that will require Google to provide additional data for time period(s) and locations that fall outside of the Initial Search Parameter(s).

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

4. Google shall disclose to the government identifying information, as defined in 18 U.S.C. § 2703(c)(2), for the Google Accounts associated with each device ID appearing on the Device List that the government has identified.

This warrant does not authorize the disclosure or seizure of any email communications or messages (SMS text or Google chat).

II. Information to Be Seized

All information described above in Section I that constitutes evidence of violations of 18 U.S.C. 111 (a)(1) that have been committed on April 25, 2023, involving unknown person(s).

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Google LLC, and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Google LLC. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Google LLC, and they were made by Google LLC as a regular practice; and

b. such records were generated by Google LLC electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Google LLC in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Google LLC, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

_____ _____

Date Signature